

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Richmond Division

IN THE MATTER OF THE SEARCH OF:

The Infotainment/Telematics Systems Contained
within the 2016 Hyundai Santa Fe Sport 2.0T
Bearing VIN 5XYZWDLA4GG340595,
Currently Located at 9325 Discovery Boulevard,
Manassas, Virginia

Case No. 3:20-sw-227



**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Christopher Drew Truslow, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant, 1) authorizing the seizure of a gray 2016 Hyundai Santa Fe Sport 2.0T, bearing VIN 5XYZWDLA4GG340595, (the “Target Vehicle”), a description of which is contained in Attachment A, and 2) authorizing the extraction and forensic examination of electronically stored information within the Target Vehicle’s infotainment/telematics systems, as particularly described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been since September 15, 2019. Prior to joining the FBI I was a Department of Criminal Justice Services certified law enforcement officer in the Commonwealth of Virginia for over fourteen years. I have participated in numerous criminal investigations including those involving fraud and identity theft.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. As set forth below, there is probable cause to believe that individuals both known and unknown have committed violations of federal criminal law, including aiding and abetting (18 U.S.C. § 2), identity fraud (18 U.S.C. § 1028), aggravated identity theft (18 U.S.C. § 1028A), mail fraud (18 U.S.C. § 1343), wire fraud (18 U.S.C. § 1343), conspiracy to commit mail and wire fraud (18 U.S.C. § 1349), money laundering (18 U.S.C. § 1956(a)(1)), and conspiracy to commit money laundering (18 U.S.C. § 1956(h)) (hereafter the “Subject Offenses”). Moreover, there is also probable cause to search the Target Vehicle described in Attachment A for evidence, instrumentalities, and/or contraband of the Subject Offenses as described in Attachment B.

PROBABLE CAUSE

5. My basis for believing that evidence is located within the Target Vehicle’s infotainment/telematics systems is as follows:

6. This investigation involves a fraud scheme that is currently fashionable and being perpetrated by multiple criminal groups both nationally and internationally. To execute the scheme, the conspirators used a variety of fraudulent scenarios to engage victims. The scheme often started with automated, previously recorded phone calls, commonly referred to as “robocalls,” which contained messages designed to create a sense of urgency with unsophisticated and/or unsuspecting recipients. These messages told the recipients that they had some sort of serious legal problem. Often the purported problem related to potential criminal charges for the victim, tax problems, or the risk of losing a federal benefits program such as

Social Security payments. Victims were informed that if they did not act immediately in accordance with the demands of the callers then there would be drastic consequences. These consequences included threats of immediate arrest and/or significant financial penalties. Some call recipients were instructed that in order to prevent these dire consequences they should call a particular phone number for further instruction.

7. When a conspirator would speak with the victim and identify themselves as a government official, the conspirator would reinforce the need for the victim to take immediate action to avoid consequences. Conspirators tricked and coerced victims to send cash to an address, supposedly belonging to a law enforcement or other government agency, as a demonstration of good faith while the criminal investigation was ongoing. In schemes involving supposed potential criminal charges, victims were assured that if they were cleared of involvement in criminal activity after a thorough investigation then their money would be returned to them.

8. In another scenario, a conspirator would contact a victim posing as a loan officer offering to provide the victim a loan. A number of victims defrauded in this scenario had recently applied for loans from legitimate lenders. The conspirator would eventually inform the victim that they had been approved for the loan, and that the loan was being deposited into the victim's bank account. In return for receipt of this purported loan, the conspirator instructed the victim to send money back as directed as a demonstration of good faith or as a loan payment.

9. Yet another technique used by the perpetrators was to contact a victim to offer maintenance assistance with their home computer, convincing the victim that there was a problem with their home computer. Sometimes this was done by tricking the victim into downloading software that perpetrators used to actually create problems with the victim's

computer. The perpetrator would then inform the victim that in order for their computer to be repaired the victim would have to send money as directed by the conspirator.

10. Some victims were directed by a conspirator to send cash via the mail or a parcel delivery service. These victims were instructed to send the bulk cash via FedEx, UPS and/or the U.S. Postal Service (“USPS”) using shipping methods that provided tracking numbers, and further to provide the tracking numbers of their shipments to members of the conspiracy. Conspirators directed other victims to send money via a wire service. These victims were instructed to send money via Western Union, MoneyGram and/or Walmart to Walmart money transfer, and further to provide the reference number for the wire transfer to members of the conspiracy.

11. Members of the conspiracy commonly referred to as “money mules” would pick up the bulk cash shipments sent to the fraudulent law enforcement addresses, often presenting counterfeit identification documents incorporating stolen or fictitious identities. Money mules would similarly pick up the wire transfers from victims using the reference numbers provided by the victims. The conspiracy’s money mules would pocket some portion of cash for themselves and deposit the remaining amount in bank accounts created and/or accessed by other conspiracy members.

12. Members of the conspiracy relied heavily on WhatsApp for communicating with each other to advance their scheme. WhatsApp is a free, cross-platform communication application that may be installed on Apple, Android, and Windows cellular telephones, as well as Mac and Windows PC computers. WhatsApp enables users to communicate securely over the Internet with end-to-end encryption using a variety of formats, including video, voice calls, and SMS (text) messaging.

11. Throughout the course of this investigation, multiple arrests have been made. For example, on December 11, 2019, pursuant to an arrest warrant issued by the United States District Court for the Eastern District of Virginia, Richmond Division, the FBI arrested Shehzadkhan Khandadkhan Pathan (hereafter “PATHAN”), at a Walmart located in Houston, Texas. Agents identified an Apple iPhone 11 Pro cellular telephone on his person at the time of arrest and subsequently seized it. PATHAN gave consent to search the cellular telephone and signed FBI Form FD-26 – Consent to Search. Notwithstanding PATHAN’s signed consent to search the iPhone, on December 13, 2019, the FBI obtained a search warrant for PATHAN’s above-referenced cellular telephone issued by the United States District Court for the Southern District of Texas. On January 8, 2020, a grand jury sitting in the Eastern District of Virginia, Richmond Division, returned a three-count indictment against PATHAN and two co-conspirators, case number 3:19-cr-00160-HEH. All three defendants were charged in Count One with conspiracy to commit mail and wire fraud, in violation of 18 U.S.C. § 1349, and in Count Two with mail fraud and aiding and abetting, in violation of 18 U.S.C. §§ 1341 and 2. PATHAN and one of the co-conspirators were also charged in Count Three with aggravated identity theft, in violation of 18 U.S.C. § 1028A.

12. Pursuant to the above-referenced search warrant obtained on December 13, 2019, the FBI continues to review PATHAN’s cellular telephone on his person at the time of his arrest. To date, the search of PATHAN’s cellular telephone has identified substantial communications between PATHAN and Pradipsinh Dharmendrasinh Parmar (hereafter “PARMAR”) via WhatsApp. PATHAN’s and PARMAR’s WhatsApp communications indicate that PARMAR, at PATHAN’s direction, used fake identifications at multiple locations around the continental United States to obtain cash sent via money transfer services, Western Union, MoneyGram, and

Walmart-to-Walmart money transfers, by victims of the above-mentioned fraud, as well as obtaining packages sent by victims containing United States currency.

13. On March 4, 2020, pursuant to an arrest warrant issued by the United States District Court for the Eastern District of Virginia, Richmond Division, the FBI arrested PARMAR while exiting the Target Vehicle in Chester, Virginia. Agents located a white Apple iPhone XS, serial number F17Y110ZKPFV, on Parmar at the time of his arrest. Agents found two other cellular telephones in the Target Vehicle, which they searched incident to PARMAR's arrest. All three cellular telephones were subsequently seized by the FBI. PARMAR gave consent to search the cellular telephones and signed FBI Form FD-26 – Consent to Search. At the time of his arrest, PARMAR was known to have been operating the Target Vehicle since at least May 2019.

14. Subsequent to PARMAR's arrest, the FBI contacted the rightful owner of the Target Vehicle to discuss PARMAR's possession and use of it. The owner stated that PARMAR has been in legal possession of the Target Vehicle since March 2019, when the owner and PARMAR made an arrangement in which PARMAR would take possession of the Target Vehicle as long as he paid the monthly car payments. To the owner's knowledge, PARMAR had been making payments for the Target Vehicle and had been the sole possessor of the Target Vehicle since March 2019. According to the vehicle's owner, the Target Vehicle had approximately 35,000 miles on the odometer when PARMAR took possession of the Target Vehicle per the rightful owner, and the Target vehicle had approximately 113,000 miles on the odometer at the time of PARMAR's arrest. During the use of the Target Vehicle, PARMAR averaged 6,500 miles per month or 78,000 miles for the duration of his use of the Target Vehicle.

15. The FBI has also discovered evidence that suggests PARMAR was using the Target Vehicle to conduct the above-referenced criminal activity. PATHAN's cellular telephone included WhatsApp messages in which PARMAR sent PATHAN photographs and videos depicting PARMAR driving to various locations, obtaining FedEx packages containing money sent by victims to various addresses, and then opening such packages and counting the money. For example, on March 15, 2019, PARMAR sent PATHAN a video of a FedEx package being opened and the enclosed money being counted by an unidentified male sitting in the driver's seat of a vehicle matching the description of the Target Vehicle. In his custodial interview subsequent to his arrest, PARMAR confirmed that he was the driver counting the money and that he was sitting in the Target Vehicle at the time.

16. Furthermore, a confidential human source for the FBI stated that PARMAR drove a dark gray SUV with Pennsylvania tags (i.e., matching the description of the Target Vehicle) when involved in retrieving packages related to Indian scam calls in or around Edison, New Jersey, in May and June 2019. The confidential human source has met with investigators on multiple occasions for face-to-face meetings. As part of standard protocols for interviewing witnesses and sources, investigators advised the source on more than one occasion of the potential criminal consequences for knowingly providing false information to investigators, which the source acknowledged understanding. The source has provided considerable information that investigators confirmed through subsequent investigation to be true. To give one example, the source identified an address being used by PARMAR and/or his co-conspirators to receive packages containing victim money. As a result, investigators were able to intercept the package and return the money to the victim. And of course, the source's information that PARMAR was driving an SUV with Pennsylvania tags was confirmed by

investigators when they arrested PARMAR, who confessed to the activity described by the source.

17. The Target Vehicle is a 2016 Hyundai Santa Fe Sport 2.0T and it is equipped with infotainment/telematics systems. As described in detail below, electronic data, information, and images stored on these systems may be successfully extracted from the Target Vehicle using proprietary hardware and software developed by a private company by the name of Berla, Inc. (hereafter “Berla”). In order to use Berla’s software, a law enforcement agent must complete Berla’s training program (a 5-day, 40-hour course) and pass two certification programs.

17. Currently, the Target Vehicle is in the lawful possession of the FBI at the FBI’s Northern Virginia Resident Agency, located at 9325 Discovery Boulevard, Manassas, Virginia 20109. The Target Vehicle has remained in FBI custody since PARMAR’s arrest (i.e., on March 4, 2020), while the FBI awaits the arrival of the rightful owner to take custody of the vehicle.

18. Finally, I know that the Target Vehicle’s infotainment/telematics systems have been stored in a manner in which the contents are, to the extent material to this investigation, in substantially the same state as they were when the Target Vehicle first came into the FBI’s possession.

**TECHNICAL BACKGROUND REGARDING CONNECTED CARS AND
INFOTAINMENT/TELEMATICS SYSTEMS IN AUTOMOTIVE VEHICLES**

19. Based on my training and experience, as well as discussions with other experienced law enforcement officers and witnesses, I have learned that the following about modern, computer-equipped vehicles with “Telematic” and “Infotainment” systems :

- a. Many modern automotive vehicles (“connected cars”) are equipped with sensors, cameras,¹ transmitters, and electronic control units (ECUs)² to monitor and manage vehicle operations, track vehicle movement, and exchange information with other vehicles and infrastructure.³ These systems also enable connected cars to interface with various types of mobile devices to facilitate the use of web-based applications, including third-party navigation, wireless telephone, multimedia streaming, and the like. To perform these computing functions, connected cars collect and process significant volumes of data.
- b. Two commonly installed ECUs within connected cars are infotainment and telematics systems—sometimes referred to as the Telematics Control Unit (TCU) and the Infotainment Control Unit (ICU). These systems typically retain large amounts of user data within the vehicle.
- c. A vehicle’s infotainment system combines hardware and software to provide entertainment features. Infotainment systems allow drivers and passengers to connect their handheld, electronic devices to the vehicle and Internet. When

¹ By law, new vehicles sold in the United States must have backup cameras installed by the manufacturer. Cameron Gulbransen Kids Transportation Safety Act of 2007, Pub. L. No. 110-189, H.R. 1216, 110th Cong. (2008).

² An ECU is a generic term applied to any embedded computer that controls one or more electrical systems within a vehicle. ECUs are typically installed in a vehicle by the original equipment manufacturer (OEM) during the manufacturing process. There are many types of ECUs, and as vehicles have more features each year, the number of ECUs in each connected car increases. Newer connected cars can integrate as many as 150 ECUs, ensuring, in theory, that each part of the vehicle is running properly. Some examples of common ECUs include the Engine Control Module (ECM), Transmission Control Module (TCM), Brake Control Module (BCM), and Suspension Control Module (SCM), as well as the Telematics Control Unit (TCU) and Infotainment Control Unit (ICU).

³ The infotainment/telematics systems in connected cars are not the same as “black box” recorders. Black box recorders are called event data recorders (EDRs) or crash data recorders (CDRs). These black box recorders can record vehicle speed, engine speed, steering angle, throttle position, braking status, force of impact, seatbelt status, and airbag deployment. In 2006, the US National Highway Traffic Safety Administration (NHTSA) adopted regulations requiring EDRs to uniformly collect certain crash data to assist crash investigators with accident reconstruction efforts. In 2012, NHTSA proposed requiring manufacturers to install EDRs in all new cars and trucks, but in 2019, the NHTSA withdrew the proposal because automakers have voluntarily installed the devices in nearly all vehicles. Black box recorders are likely only going to be of use in cases where there has been a crash of some kind.

connected, the driver and passenger may gain access to, for example, Global Positioning System (GPS) navigation, video players, music streaming, voice calling, texting, and traffic data. Drivers can talk hands-free with Bluetooth connectivity, listen to music, watch videos, or pull up a mapped route to their chosen destination. This is all possible via the (typically interactive) console located on the front dashboard of the vehicle.

- d. A vehicle's telematics system collects and stores diagnostic data from various systems (other ECUs) within the vehicle, including historical navigation points, speed, and event data. Historical event data may include information regarding when the car's trunk, doors, and windows opened and closed, when headlights turned on and off, and when gears change or brakes were engaged.
- e. The main difference between the infotainment and telematics systems is that the infotainment system is about entertainment for the occupants of the vehicle, and the telematics system is for collecting and reporting (transmitting) information—such as vehicle use data, maintenance requirements, and automotive servicing—about the vehicle. Typical telematics data may include turn-by-turn navigation, remote access, emergency calling, and maintenance notifications. The first vehicle telematics system was General Motors' OnStar. OnStar started as a subscription-based service that promised in-vehicle security, hands-free calling, remote diagnostics, and emergency services. Other, newer examples include BMW's "Assist" and Mercedes' "mbrace." Some of these systems are integrated multimedia navigation and telematics systems in one (combined infotainment/telematics systems), like Toyota's "Entune" and Ford's "Sync."
- f. The data generated, collected, transmitted, and retained by connected cars can provide valuable information in law enforcement investigations of crimes. For example, many infotainment systems support the importation of content and other data information from a particular user's mobile device. Such data may include content that may provide attribution to particular user(s), including mobile device identifiers, wireless telephone numbers, user account details, methods of payment, passwords, user voice profiles, contact lists, call logs, text messages, pictures, e-mail, videos, web history, GPS coordinates, and other historical navigation information.
- g. I am aware that the computers (ECUs) within many connect cars store data for prolonged periods of time. Furthermore, even after a previously-connected mobile device is removed from the physical vehicle, much of the logical data—and some deleted data—may remain within the digital storage of the system.

Such stored data can be used to identify locations, victims, witnesses, associates, and co-conspirators and may include communications and images of criminal activity. In sum, a forensic examination of a connected car's infotainment/telematics systems may reveal the vehicle's GPS location information, movements, operations, and user data at critical moments before, during, and after the commission of a crime.

- h. As previously stated, the Target Vehicle is a Hyundai Santa Fe Sport 2.0T. I know that the Target Vehicle is supported by Berla's software because I have searched the Target Vehicle's VIN in Berla's vehicle lookup database that confirmed it is supported. To complete a forensic extraction from the Target Vehicle, it may be necessary, temporarily, to remove trim and other components of the Target Vehicle to access the infotainment/telematics systems. It may also be necessary to repair the device, replace the screen, reconnect wires, and replace batteries. It may be necessary to employ advanced forensic processes to bypass locked display screens and other data access restrictions. Advanced processes may include potentially destructive processes such as JTAG, chip-off, and ISP, which are forensic techniques used to remove memory chips from computers and other electronic storage containers that may be found within the Target Vehicle. *To the extent that destructive processes would be necessary to forensically extract data from the Target Vehicle, investigators will not use such destructive processes.*
- i. Furthermore, it may be necessary to return to the Target Vehicle and reconnect the infotainment/telematics systems to the Target Vehicle's power source to perform the extraction using Berla, Inc.'s software. This is because there are various computer networks working simultaneously when a vehicle is powered on, and in some vehicles, the infotainment/telematics systems require the other networks to work in tandem to complete the data extraction.
- j. Finally, a full search and review of all the data retrieved from the infotainment/telematics systems of the Target Vehicle may not be completed within 14 days. Searching electronic storage and communication devices often requires that the search be completed by a qualified person because of the volume of evidence and technical requirements of the forensic examination.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Electronic Control Unit: An electronic control unit (ECU) is a generic term applied to any embedded computer that controls one or more electrical systems within a vehicle. ECUs are typically installed in a vehicle by the original equipment manufacturer (OEM) during the manufacturing process. There are many types of ECUs, and as vehicles have more features each year, the number of ECUs in each connected car increases. Newer connected cars can integrate as many as 150 ECUs, ensuring, in theory, that each part of the vehicle is running properly. Some examples of common ECUs include the Engine Control Module (ECM), Transmission Control Module (TCM), Brake Control Module (BCM), and Suspension Control Module (SCM), as well as the Telematics Control Unit (TCU) and Infotainment Control Unit (ICU).
- c. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard

drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.


- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of a minimum of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
 - e. Tablet: A tablet is a mobile computer, typically larger than a phone, yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 “Wi-Fi” networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
 - f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.
21. Based on my training, experience, and research, I know that the Target Vehicle has capabilities that allow it to connect to and download data from electronic devices such as smartphones, which have the capability of acting as a wireless telephone, portable media player, digital camera, GPS navigation device, etc. In my training and experience, examining data stored

on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and therefore, was likely within the Target Vehicle.

CONCLUSION

22. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Target Vehicle's infotainment/telematics systems as described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,




Christopher Drew Truslow
Special Agent
Federal Bureau of Investigation

Subscribed and sworn by the affiant in accordance with the requirements of Fed. R. Crim.

P. 4.1 by telephone

on July 1, 2020:



/s/
Roderick C. Young
United States Magistrate Judge

UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
(Property To Be Searched)

The property to be searched is the infotainment/telematics systems within a gray 2016 Hyundai Santa Fe Sport 2.0T, bearing VIN 5XYZWDLA4GG340595 (the “Target Vehicle”). The Target Vehicle is currently located at the FBI’s Northern Virginia Resident Agency, located at 9325 Discovery Boulevard, Manassas, Virginia 20109.

This warrant authorizes the forensic examination of the Target Vehicle’s infotainment/telematics systems for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B
(Items to be Seized)

1. Any and all records on the Target Vehicle's infotainment/telematics systems relating to violations of including aiding and abetting (18 U.S.C. § 2), identity fraud (18 U.S.C. § 1028), aggravated identity theft (18 U.S.C. § 1028A), mail fraud (18 U.S.C. § 1343), wire fraud (18 U.S.C. § 1343), conspiracy to commit mail and wire fraud (18 U.S.C. § 1349), money laundering (18 U.S.C. § 1956(a)(1)), and conspiracy to commit money laundering (18 U.S.C. § 1956(h)) (hereafter the "Subject Offenses"), those violations involving **Pradipsinh**

Dharmendrasinh Parmar, Shehzadkhan Khandadkhan Pathan, and their conspirators, both known and unknown, to include **but not limited to the following including:**

- a. communications or documents relating to the movement of packages or money, including but not limited to shipments by commercial parcel carriers to include the U.S. Postal Service, UPS, FedEx, and DHL;
- b. communications or documents relating to money transfers by wire services, including but not limited to Western Union, MoneyGram and Walmart-to-Walmart money transfers;
- c. communications or documents involving fictitious identification cards;
- d. communications or documents involving any United States agency or police department, including but not limited to the United States Treasury, Internal Revenue Service, Drug Enforcement Agency, or Social Security Administration;
- e. travel or location information;
- f. bank records, checks, credit card bills, account information, virtual currency, and other financial records;
- g. evidence of user attribution showing who used or operated the Target Vehicle or mobile devices that interfaced with its infotainment/telematics systems at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;
- h. records of Internet activity, including firewall logs, internet protocol addresses, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

- i. evidence of the times the Target Vehicle or mobile devices that interfaced with its infotainment/telematics systems were used;
- j. records or information related to social media accounts, email accounts, communication accounts, or cloud based accounts;
- k. photos, audio files, or video files;
- l. SIM card information;
- m. notes, reminders, SIRI commands or questions, or device settings;
- n. activity, connection, and transactional logs including but not limited to FaceTime, iMessages, text messages, mail logs, iCloud logs, iTunes Store and Apple Store logs, My Apple ID and Find iPhone logs, Game Center logs, call logs, and logs associated with purchase, activation, and upgrade of mobile devices that interfaced with the Target Vehicle's infotainment/telematics systems;
- o. documentation and manuals that may be necessary to access the Target Vehicle's infotainment/telematics systems or to conduct a forensic examination of the systems;
- p. evidence indicating the user's state of mind as it relates to the crime under investigation;
- q. evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts; and
- r. passwords, encryption keys, and other access devices that may be necessary to access the Target Vehicle's infotainment/telematics systems.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and

technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.